



2014

# Emerging Identity Theft and Fraud Initiatives

Jodi Patterson, Director  
Return Integrity and  
Correspondence Services



# Agenda

---

- Device ID Overview
- Limiting Multiple Direct Deposits Overview

# Device ID



## Why Implement Device ID?

- Software companies, internal, and external stakeholders have suggested additional measures to combat fraud
- Capturing of Device ID was proposed to IRS by the American Coalition for Taxpayer Rights in December 2012
- Software companies and private industry already capture device identification information and notifies taxpayers of such in the Privacy Statements
- The IRS is committed to maintaining taxpayer privacy

## Device ID Effect on Fraud

- Device ID can assist in combatting fraud through the following methods:
  - **Increased Detection:** A large volume of fraudulent returns are identified by pattern matching and trends. Device ID will enable the IRS to easily associate fraudulent returns that are filed from the same device.
  - **Improved Effectiveness of Fraud Detection:** Device ID can be more unique than an IP address and can be more effective in fraud detection when used in conjunction with an IP address. A device can have several IP addresses; however, the Device ID should be unique.
  - **Negative Impact for Criminals:** Once a device is identified as filing fraudulent returns, the device can be flagged to allow the IRS to identify additional fraudulent returns more readily. The IRS is discouraging future fraud by increasing the potential cost to commit tax fraud. If a criminal chooses to continue, after a device has been identified and refunds stopped, significant risks of identification are incurred. The criminal will need to purchase additional equipment in an effort to go undetected.
  - **Decreased Taxpayer Burden:** Device ID has a high benefit and a minimal burden to the taxpayer. The Device ID will be submitted seamlessly with the return via existing electronic return transmission processing. Device ID requires little to no action from the taxpayer. Furthermore, fraud is often committed using stolen SSNs. By putting in place measures to identify fraud and treat it, the IRS combats ID theft and prevents downstream impact of ID theft on IRS and good taxpayers.



## **Device ID is an IRS Initiative to Improve the Service's Ability to Identify and Reduce Refund Fraud**

---

- A unique identification number (Device ID) will be developed and transmitted as part of each electronically filed return
- The key objectives of the Device ID Initiative are to:
  - Increase the Service's ability to identify and reduce fraud
  - Support non-compliant and fraud identification processes
  - Reduce the total dollars of improper payments
  - Expedite the processing of compliant returns
  - Support revenue protection strategies
  - Protect taxpayers who may fall victim to fraud



## **This unique ID will be transmitted as part of the electronically filed return via our existing transmission processes**

---

- The IRS will not have access to, or store, any device serial numbers
- The masked results cannot be reversed to determine the serial number
- Notice of the use of these procedures will be provided to taxpayers in e-file transmitter guidelines (Publication 1345) and system of records notices (SORN) that are published in the Federal Register



## **The unique device ID data will be accessed and developed into the software industry programming**

---

- The programming will request the serial number of the device (Computer, Smart Phone, Tablet) used to submit an electronically filed return
- The serial numbers will be obtained and masked, using the hashing algorithm, as part of the industry's software programming
- A hash algorithm will be applied to the unique serial number to derive a hash total, this hash total will in fact be the specific "Device ID" or fingerprint for the purposes of electronically filing returns
- This unique ID will be transmitted as part of the electronically filed return via our existing transmission processes



## **Secure Hash Algorithm (SHA – 1) is the Proposed Algorithm for Programming the Device ID**

---

- Secure and on National Institute of Standards and Technology (NIST) List of approved hashing algorithms that meet security standards
- Low impact to developers because of easy implementation and current widespread availability across a wide range of devices and operating systems
- Low impact to taxpayers because hashing algorithm is not time consuming



## Consistent Programming is Required Across All Platforms Used to Transmit Electronic Returns

---

- IRS will work with software developers to ensure consistent programming for the various platforms:
  - Mobile devices
  - Tablets
  - Web Browsers
  - Windows
  - MAC

### **Two Types of Software Will Require Programming**

- Application to Application (software programs)
- Internal Filing Application (web browser)



## Proposed Information Captured from MAC and Windows Based Systems

---

- Obtain Primary hard drive serial number and UUID from device
- Concatenate serial number and UUID together with no separators and run string of characters through the algorithm and submit the information to the IRS

# Requirements of Hashed Data for all Platforms

---

- Consistent information selected from software across platforms to ensure hashing results are the same regardless of the platform
- Use of unique information to ensure no duplicate device ids are created for the same device



## Information/Actions Needed from Software Developers

---

- Name of all platforms that you use in addition to Windows and MAC to transmit returns
- Unique information that can be captured from each platform to be hashed and transmitted to the IRS
- Test hashing accuracy to ensure software has properly hashed the device id prior to submittal of information to the IRS

## Questions?

- The IRS developed a mailbox for software industry representatives to submit questions during Device ID implementation:  
***wi-rics.device.id@irs.gov***

# Limiting Multiple Direct Deposits



## Initiative to Limit the Number of Tax Refund Checks Deposited Into a Single Bank Account

---

- **Background** - Except in limited circumstances, Treasury and Internal Revenue Service (IRS) rules prohibit the deposit of individual tax refund checks into a business account and prohibit return preparers from endorsing or otherwise negotiating an individual tax refund check.
- **Impact Analysis** - Data analysis of tax returns filed in Processing Year (PY) 2013 indicates that out of 65 million tax returns with requests for direct deposit, 3.4 million had multiple refunds going to a single bank account
  - Data shows multiple refunds deposited to a single account is an indication of fraudulent or ID theft activity on the tax return because it is easy for the perpetrator to establish and retrieve direct deposits from a single account.
- **Initiative** - Beginning in January 2015, we will limit the number of tax refund deposits to a single account to three (3). We will flip refunds to paper checks when the number of deposits exceeds three. We believe this initiative will have a positive impact on our efforts to deter fraud and identity theft. Stakeholders such as Treasury Inspector General for Tax Administration (TIGTA), Treasury Fiscal Services, Banking Industry, Practitioner community and Congress have expressed strong support of this effort.



# Questions?